

UD1_T6 Antivirus



Índice

1. Analizar el antivirus Windows Defender.....	3
2. Copia los ficheros adjuntos a la actividad y comprueba si Windows Defender detecta amenazas..	4
3. Utiliza la web de virustotal para analizar los ficheros adjuntos a la actividad. Documenta el procedimiento.....	5

1. Analizar el antivirus Windows Defender.

Realiza una comprobación del equipo (rápida) y anota estos puntos:

- Número archivos analizados.
- % Ocupación de CPU en ejecución.
- Tiempo de escaneo.
- Vulnerabilidades y virus encontrados y desinfectados.

Protección antivirus y contra amenazas

Protección contra amenazas para tu dispositivo.

Amenazas actuales

Ejecutando examen rápido...
Tiempo restante estimado: 00:00:00
45190 archivos examinados

Cancelar

Puedes seguir trabajando mientras se ejecuta el examen.

[Historial de protección](#)

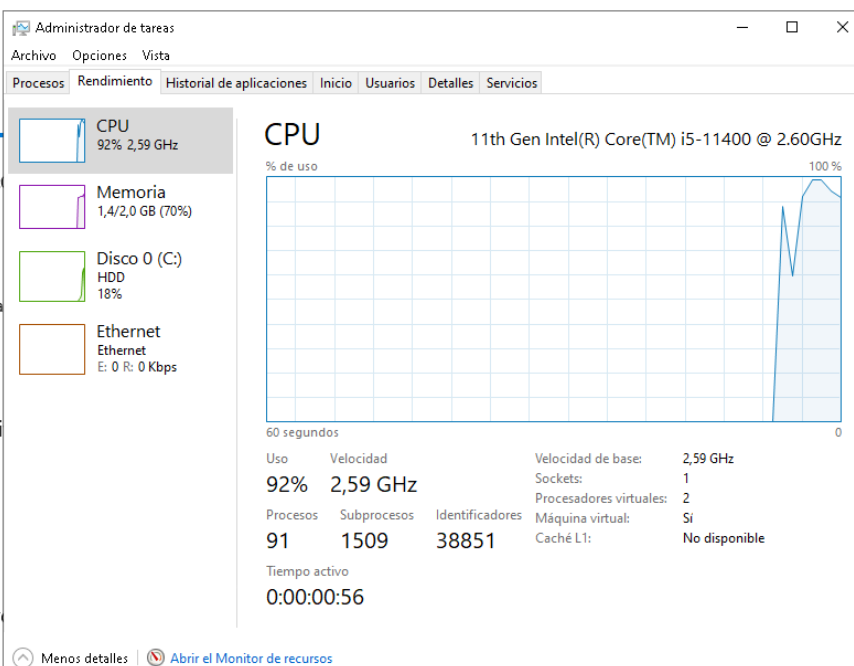
Configuración de anti amenazas

No se requiere ninguna acción.

[Administrar la configuración](#)

Actualizaciones de protección

La inteligencia de seguridad está actualizada.



Protección antivirus y contra amenazas

Protección contra amenazas para tu dispositivo.

Amenazas actuales

No hay amenazas actuales.

Último examen: 13/10/2023 8:59 (examen rápido)

Se encontraron 0 amenazas.

El examen duró 3 minutos 34 segundos

31802 archivos examinados.


Examen rápido

[Opciones de examen](#)

[Amenazas permitidas](#)

[Historial de protección](#)

2. Copia los ficheros adjuntos a la actividad y comprueba si Windows Defender detecta amenazas.



Se encontró una amenaza. Es necesario realizar alguna acción.

13/10/2023 9:15

Alta ^

Detectado: Misleading:Win32/Lodi

Estado: Activo

Las amenazas activas no se han corregido y se están ejecutando en el dispositivo.

Fecha: 13/10/2023 9:15

Detalles: Este programa muestra mensajes engañosos de productos.


Elementos afectados:

containerfile: C:\Users\admin\Desktop\REVEALER KEYLOGGER 2.2 full crack ojo virus.rar

file: C:\Users\admin\Desktop\REVEALER KEYLOGGER 2.2 full crack ojo virus.rar->REVEALER KEYLOGGER 2.2\Instalador\REVEALER KEYLOGGER_2.2.exe

[Más información](#)

Acciones ▾



Amenaza en cuarentena

13/10/2023 9:15

Grave ^

Detectado: MonitoringTool:Win32/RevealerKeylogger

Estado: En cuarentena

Los archivos en cuarentena se encuentran en un área restringida donde no pueden dañar el dispositivo. Se eliminarán automáticamente.

Fecha: 13/10/2023 9:15

Detalles: Este programa supervisa la información del usuario.

Elementos afectados:

file: C:\Users\admin\Desktop\rkfree_setup_301_password_123.zip

[Más información](#)

Acciones ▾

3. Utiliza la web de virustotal para analizar los ficheros adjuntos a la actividad. Documenta el procedimiento.

4
/ 62

Community Score

4 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

4907b3f1e4a02f1f59c8030da43d79083aa14f219f7c583a7844c41aa87880db9

Size751.89 KB

Last Analysis Date4 months ago

ZIP

rkTree_setup_301_password_123.zip

zipencrypted

DETECTION

DETAILS

COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

Threat categories

Family labels

Community Score

Security vendors' analysis

Do you want to automate checks?

Fortinet	Riskware/RevealerKeylogger	Microsoft	MonitoringTool:Win32/RevealerKeylogger
NANO-Antivirus	Riskware.Win32.Keylogger.juojpt	Symantec	PUA.Superfluous
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected

Basic properties

MD5c82f73b373309619c3765eb9dea72263

SHA-1a23dbcb53f80377aa0217aacc1241ead5a5294af

SHA-256ae333d10c23ef228fb4cff543db1b808d26a9dd5a37d6a302d5392f55e777ffa

Whaash1015a82b15f7c9502858c4ccca4aa930

SSDEEP24576rNawwaQIMPGZdbFuX3dhtzJRCJjIXAh6v5w7+F8fUcpgJF2qvwZLYkvMprN+ZBFudfxJRp0ZvSX8M40YV

File typeRAR compressedrar

MagicRAR archive data, v1d, os: Win32

TrIDRAR compressed archive (v~4~) (58.3%) | RAR compressed archive (gen) (41.6%)

File size1.42 MB (1486792 bytes)

History

First Seen In The Wild2017-05-22 16:22:42 UTC

First Submission2017-06-20 00:25:03 UTC

Last Submission2023-10-13 07:28:30 UTC

Last Analysis2018-11-07 18:44:12 UTC

Earliest Contents Modification2017-03-31 08:49:46

Latest Contents Modification2017-05-22 11:20:45

Names

REVEALER KEYLOGGER.22.full.crack.o.p.virus.rar

REVEALER KEYLOGGER.22.rar

REVEALER KEYLOGGER.22.full.crack.o.p.virus (1).rar

Bundle info

Contents Metadata

Contained Files10

Uncompressed Size1.57 MB

Earliest Content Modification2017-03-31 08:49:46

Latest Content Modification2017-05-22 11:20:45

Contained Files By Extension

21

EXE1

TXT2

URL5



Community Score

24 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

ee333d10c23ef228fb4cff543db1b808d26a9dd5e37d6e302d5392f55e777ffa
REVEALER KEYLOGGER 2.2.rar

Size
1.42 MB

Last Analysis Date
5 years ago



DETECTION DETAILS COMMUNITY 1

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label pua.revealerkeyloggerkeylogger

Threat categories pua trojan

Family labels revealerkeylogger keylogger monitor

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	RiskWare[Monitor]/Win32.RevealerKeylo...	Arcabit	Application.Generic.D526345
BitDefender	Application.GenericKD.5399365	ClamAV	Win.Trojan.Agent-6244858-O
Cyren	W32/Application.HSAR-3240	Emsisoft	Application.GenericKD.5399365 (B)
eScan	Application.GenericKD.5399365	ESET-NOD32	A Variant Of Win32/KeyLogger.RevealerK...
F-Secure	Application.GenericKD.5399365	Fortinet	Riskware/RevealerKeylogger
GData	Application.GenericKD.5399365	Ikarus	PUA.KeyLogger.RevealerKey/logger
Jiangmin	Monitor.RevealerKeylogger.i	K7AntiVirus	Password-Stealer (D050e64c1)
K7GW	Password-Stealer (D050e64c1)	Kaspersky	Not-a-virus:Monitor.Win32.RevealerKeyl...

Basic properties

MD5 02e035ab50c0887ef48da99eb1f8cf8a
SHA-1 ea4105d9c7b50f1384f0c05611a79e5a3d1f95aa82
SHA-256 4f0703f1e4a20f157e2b0306a43d79c83ae4f219f7c583a7844cd1aa87880db9
Virushash 8a22546c3450e07070929f2f5aa8298f6
SSDEEP 12289:FWJdH8KFWb15yW16P7oEAFD2KUKx3Jd5ZPhPG6rHmHuUwz+1qPjkZTuFGSjrdw4JN7vAFaKDXdzdf6UthpG
TLSH 1147f42257809FEF38A7063AF07578A3A87Aa6814CC1F07986778E5F44198B503C908BCA
File type ZIP compressed zip
Magic Zip archive data, at least v2.0 to extract, compression method=deflate
TrID Zip compressed archive (8.0%) PrintFoxPagefox bit map (640x800) (2.0%)
File size 751.89 KB (769934 bytes)

History

First Seen In The Wild 2021-06-25 18:31:52 UTC
First Submission 2021-06-12 16:46:50 UTC
Last Submission 2023-10-13 07:31:03 UTC
Last Analysis 2023-06-31 23:27:20 UTC
Earliest Contents Modification 2021-06-10 11:33:26
Latest Contents Modification 2021-06-10 11:33:26

Names

rfree_setup_301_password_123.zip
f_0016d2
rfree_setup_301_password_123 (1).zip
Keylogin_password_123.zip
rfree_setup_301_password_123.QdRlH6TB.zip.part
rfree_setup_301_password_123.PPstDWWd.zip.part
bf914882-a225-433c-8449-b69a42b51eaa.zip
N5o confirmedo 129975.cdownload

Bundle Info

Contents Metadata

Contained Files 1
Uncompressed Size 179 MB
Earliest Content Modification 2021-06-10 11:33:26
Latest Content Modification 2021-06-10 11:33:26

Contained Files By Extension

EXE 1